

Two-dimensional distributed-phase-reference protocol for quantum key distribution

Davide Bacco,^{1,*} Jesper Bjerger Christensen,¹ Mario A. Usuga Castaneda,¹ Yunhong Ding,¹ Søren Forchhammer,¹ Karsten Rottwitt,¹ and Leif Katsuo Oxenløwe¹

¹Technical University of Denmark, Department of Photonics, 2800 Kgs. Lyngby, Denmark.

Quantum key distribution (QKD) and quantum communication enable the secure exchange of information between remote parties. Currently, the distributed-phase-reference (DPR) protocols, which are based on weak coherent pulses, are among the most practical solutions for long-range QKD. During the last 10 years, long-distance fiber-based DPR systems have been successfully demonstrated, although fundamental obstacles such as intrinsic channel losses limit their performance. Here, we introduce the first two-dimensional DPR-QKD protocol in which information is encoded in the time and phase of weak coherent pulses. The ability of extracting two bits of information per detection event, enables a higher secret key rate in specific realistic network scenarios. Moreover, despite the use of more dimensions, the proposed protocol remains simple, practical, and fully integrable.

INTRODUCTION

Sharing sensitive information has always been a great challenge within our society. In particular, QKD, first introduced by Bennett and Brassard, provides a unique procedure for exchanging a private key, based on the laws of quantum mechanics [1]. During the last decade, the effort from the scientific community has been focused on an enhancement of the quantum communication performances in terms of key rate, transmission distance and security aspects [2–8]. In later years this technology has matured enormously, but the lack of compact, efficient, inexpensive, and reliable systems, has restricted wide spreading of practical QKD systems.

The basic idea behind QKD systems, in the case of "prepare and measure" schemes, is based on quantum states prepared by Alice (the transmitter) and sent through a quantum channel towards Bob (the receiver). Depending on the quantum measurement, Bob can deduce which state was prepared by Alice. This way, after error reconciliation and privacy amplification methods established in a classical channel, the two users share an identical bit sequence. Ideally, QKD systems are secure with no chance for an eavesdropper to extract information on the key. However, in real implementations of the systems, due to the losses and imperfections of devices, the secret key rate defines a bound on how much information can be assumed secure [9–11].

We here propose a new QKD protocol, which we refer to by the name: Differential phase time shifting (DPTS). In its essence, the protocol utilizes two degrees of freedom — time and phase — to encode information in a quaternary alphabet, i.e. $\{0, 1, 2, 3\}$ [12]. The DPTS belongs to the family of distributed phase-reference (DPR) protocols, which rather than using the principle of random basis-choices between different mutually unbiased bases, encodes information in adjacent weak coherent pulses [9, 13, 14]. We study the performance of the DPTS protocol using infinite-key analysis in the case of collective attacks, and further show that the protocol holds great potential in intracity network scenarios.

RESULTS

Principle of DPTS

As in most practical implementations of QKD, the DPTS protocol, which is sketched in Fig. 1, uses a source of weak coherent pulses to establish a key of random numbers between two authenticated parties, Alice and Bob. To initiate the key distribution process, Alice randomly encodes information in the train of pulses in two dimensions, time and phase. *The time encoding* is performed using an intensity modulator (IM) as in the coherent-one way (COW) protocol [14]. For every pair of pulses (we refer to such a pair as a *sub-block*), one pulse is transmitted with mean photon number $\mu < 1$ ($|\alpha\rangle$), and one is blocked completely ($|\text{vac}\rangle$). Hence, within each sub-block, information is carried by the time-of-arrival of a non-empty pulse [14]. *The phase encoding* is performed using a phase modulator (PM), where a random phase between sub-blocks is either $\{0, \pi\}$. By combining the effect of the IM and the PM, Alice prepares states from the quaternary alphabet:

$$\begin{aligned} |0\rangle &= |\pm\alpha\rangle|\text{vac}\rangle|\pm\alpha\rangle|\text{vac}\rangle, \\ |1\rangle &= |\pm\alpha\rangle|\text{vac}\rangle|\mp\alpha\rangle|\text{vac}\rangle, \\ |2\rangle &= |\text{vac}\rangle|\pm\alpha\rangle|\text{vac}\rangle|\pm\alpha\rangle, \\ |3\rangle &= |\text{vac}\rangle|\pm\alpha\rangle|\text{vac}\rangle|\mp\alpha\rangle. \end{aligned} \quad (1)$$

Bob may distinguish unambiguously between these states by employing an unbalanced interferometer which interferes adjacent sub-blocks separated by $T = 2/\nu$, where ν is the laser repetition rate.

It is important to note that, analogous to the differential phase shift (DPS) protocol, each sub-block may participate in defining up to two states [13]. For instance, the sequence: $|\alpha\rangle|\text{vac}\rangle, |-\alpha\rangle|\text{vac}\rangle, |\text{vac}\rangle|\alpha\rangle, |\text{vac}\rangle|-\alpha\rangle$ encodes the states: $|1\rangle, |0\rangle, -, |2\rangle$. Here, the '-' indicates a change of the temporal sequence over the sub-block separation, in which case Bob is not able to interfere the non-empty

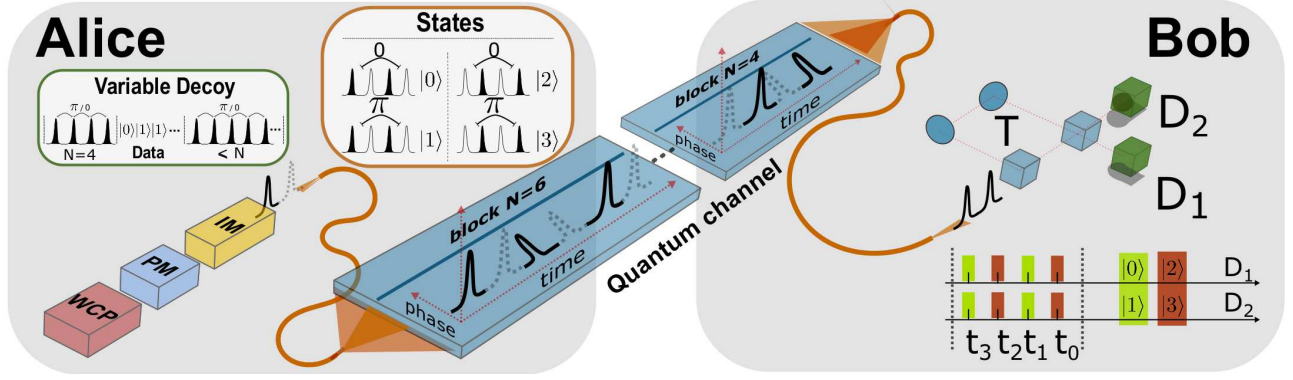


FIG. 1. *Basic scheme of the DPTS protocol.* A train of weak coherent pulses (WCP) is emitted by a laser of repetition rate ν ($2/T$), and attenuated to the single photon level. A phase modulator (PM) encodes the first key bit in non adjacent pulses choosing a random phase between 0 and π . An intensity modulator (IM), exploiting two different time positions, encodes the second key bit by randomly choosing between the time instances $|\pm\alpha\rangle|\text{vac}\rangle$ or $|\text{vac}\rangle|\pm\alpha\rangle$. The length of the block (N), in which the IM uses the same time sequence, is defined by Alice who randomly decides between different duration ($N \geq 4$). In this way Alice prepares a sequence of different states: $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. A random decoy sequence is implemented in order to check the coherence between pulses. Using a delay line interferometer (T delay between arms), the receiver, Bob, can simultaneously measure the phase and the time of arrivals of the photons.

pulses in his interferometer. Therefore, to minimize the number of unused sub-blocks (or measurements), Alice may benefit from repeating the temporal encoding over long pulse sequences (i.e. only using $|0\rangle$ and $|1\rangle$, or $|2\rangle$ and $|3\rangle$ for long intervals). However, doing so permits a potential eavesdropper, Eve, to gain partial information on a given state by measuring the time-of-arrival of pulses in adjacent sub-blocks. To take into account this possibility, Alice prepares blocks of length N , within which the temporal sequence of empty and non-empty pulses is the same. The value of N , counting both empty and non-empty pulses, is for each block chosen randomly in a uniform distribution: $N \in \{4, 6, \dots, N_{\max}\}$. This modification means that both Bob and Eve are essentially unaware of the positions of the block separations, and, whereas this is of no importance to Bob, it is fundamental for Eve.

The security of DPTS relies on the same principle as other DPR protocols: the coherence between non-empty pulses [15, 16]. Eve can not perform a measurement on any finite number of states without at some point breaking coherence between successive pulses. This is specifically true for the DPTS protocol since Eve is completely ignorant about the start and end of blocks (note that coherence is not carried across a block separation corresponding to two sub-blocks of different temporal sequences). However, since coherence is distributed across sub-block separations whereas the temporal information lies within sub-blocks, a sophisticated Eve can address each sub-block separately trying to just learn the time-of-arrival information (i.e. is a state $|0\rangle$, $|1\rangle$ or is it $|2\rangle$, $|3\rangle$). Doing so, she only breaks coherence *within* sub-blocks, and thus Bob, who only checks coherence *across* sub-blocks, is not able to reveal her presence. To counter this

attack, Alice introduces decoy sequences with probability $p_{\text{decoy}} \ll 1$ [15], in which blocks consist of N non-empty pulses. Interestingly, this decoy is just a DPS sequence in which the phase encoding is carried between every second pulse (as measured by Bob). Consequently, if Eve probes one or more sub-blocks containing two non-empty pulses, she inevitably disturbs the phase relation between these pulses [10]. As a result, there are cases where Eve introduces phase errors into the communication.

Protocol definition

We now describe in detail how Alice and Bob establish a common key using the DPTS protocol:

- Alice prepares states for transmission in the quantum channel using her phase- and intensity modulators. We assume that Alice chooses equally and randomly between the four different states $\{0, 1, 2, 3\}$. The temporal sequence is repeated within each block of random length ($N \geq 4$), whereas the phase difference between each sub-block is changed randomly between $\{0, \pi\}$.
- Once Bob has received a photon in one of the two detectors, he reveals over a public classical channel the sub-time (the number of the sub-block) instances of his recorded detection events.
- Alice reports back by telling which of the events corresponded to an overlap between adjacent blocks with opposite temporal sequence (a block separation was present in that instance). Bob must discard these events.

- For each of the remaining detection events, Alice and Bob establish two bits of information for their key: Alice easily figures out the detection time from her sent temporal sequence, and infers from her phase encoding which detector clicked at Bob's side.
- After estimating the quantum bit error rate (QBER), Alice and Bob perform standard error reconciliation and privacy amplification [17–19]. At the end of the process Alice and Bob share secure identical keys.

Secret key rate

To further describe the proposed protocol, let us consider the maximum extractable secret key rate R_{sk} [10]. For the DPTS protocol this quantity reads

$$R_{sk} = f R_B [I_{AB} - \min(I_{AE}, I_{BE})], \quad (2)$$

where $R_B = R + 4p_d(1 - R)$ is the total detection rate with $R = [1 - \exp(-\mu t \eta_d)]/2$. μ is the mean photon number of non-empty pulses, t represents the quantum channel transmission coefficient, η_d is the (common) detector efficiency, and p_d is the dark count probability. The pre-factor $f = (1 - p_{decoy})((\langle N \rangle - 1)/\langle N \rangle)$, where $\langle N \rangle$ is the average block length, takes into account the fraction of Bob's detection events that is assigned to the key string. The unused fraction $1/\langle N \rangle$ is due to detections associated with adjacent sub-blocks of different temporal sequences. In these cases, the clicks are randomly distributed between the two detectors, and so the instances are discarded.

The mutual information between Alice and Bob, is expressed in terms of the Shannon entropy as $I_{AB} = H(A) - H(A|B)$ [20]. Alice has a total of four different states to choose from, and by assuming that she prepares each state with equal probability, one finds $H(A) = -\sum_{i=1}^4 (1/4) \log_4(1/4) = 1$. Note that we, for convenience, measure information using a base-4 logarithm rather than the common base 2 [in units of bits one acquires $H(A) = 2$]. Furthermore, the conditional entropy $H(A|B)$ is expressed as

$$H(A|B) = S_4(1 - e_r^{(1)}) + \sum_{i=2}^4 S_4(e_r^{(i)}), \quad (3)$$

with $S_4(x) \equiv -x \log_4 x$, and where the four error probabilities are given as

$$\begin{aligned} e_r^{(1)} &= \frac{R \frac{1-V}{2} + 3p_d(1-R)}{R_B}, \\ e_r^{(2)} &= \frac{R \frac{1-V}{2} + p_d(1-R)}{R_B}, \\ e_r^{(3)} &= e_r^{(4)} = \frac{p_d(1-R)}{R_B}, \end{aligned} \quad (4)$$

where $V = (p_{D_1} - p_{D_2})/(p_{D_1} + p_{D_2})$ represents the visibility of the interferometer used by Bob and p_{D_1} (p_{D_2}) represents the probability of detection in detector D_1 (D_2). Note that, in the definition of the error probabilities, the visibility appears in only two of the four terms, since an interferometer error does not alter the time of arrival. As a result, the DPTS protocol is less effected by interferometer mismatches as compared to the DPS protocol. On the other hand, the higher dimensionality of the DPTS protocol renders it more vulnerable to dark counts (one dark click produces two errors on the key), effectively limiting its use at long communication distances.

In order to evaluate the achievable secret key rate for Alice and Bob, we next introduce an upper bound on the information that a potential eavesdropper might obtain by performing the most basic attack; the beam-splitting attack. A complete analysis would concentrate on I_{BE} since Eve is clueless about detection events resulting from imperfections at Bob's side [see Eq. (2)]. However, as a first attempt to estimate her information, we restrict ourselves to the more simple analysis of I_{AE} .

Security analysis

This section presents an analysis of security based on the collective beam-splitting attack (BSA) and follows the method used in [21] for the DPS and COW protocols. In the BSA, Eve replaces the quantum channel connecting Alice and Bob by a lossless line. Using a beam-splitter to simulate the losses of the quantum channel, Eve acquires $1-t$ of the signal without disturbing the state sent by Alice. Thus, the BSA belongs to the family of zero-error attacks, and is therefore undetectable by Alice and Bob. The states prepared by Alice consist of sequences $\bigotimes_k |\alpha_k\rangle$ with $\alpha_k \in \{+\alpha, 0, -\alpha\}$, so by performing the BSA, Eve receives states of the form $\bigotimes_k |\alpha_k^{(E)}\rangle$, where $\alpha_k^{(E)} \in \{+\alpha_E, 0, -\alpha_E\}$ with $\alpha_E = \alpha\sqrt{1-t}$.

At this point we assume that Eve stores the states in her quantum memory for measurement after Bob reveals his detection events. Indeed, for such a collective attack, the maximum information she may extract is given by the Holevo quantity (which must be maximized with respect to the strategies available to Eve, though here we only consider the BSA) [10, 22]

$$\chi_{AE} = S(\rho_E) - \sum_j p_j S(\rho_{E|j}) \quad (5)$$

Here S is the von Neumann entropy, $\rho_E = \sum_j p_j \rho_{E|j}$, p_j is the probability of Alice preparing the four states $j \in \{0, 1, 2, 3\}$, and $\rho_{E|j}$ is Eve's state conditioned on preparation of state j . As mentioned earlier, we consider only the balanced situation where Alice prepares each state with a probability $p_j = 1/4$. In the current protocol each value in the quaternary alphabet is encoded

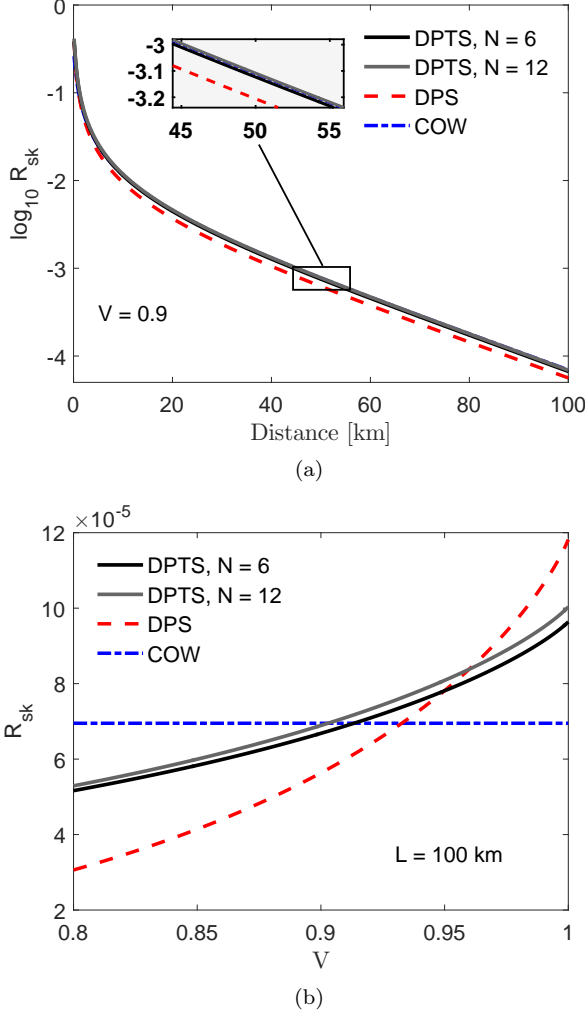


FIG. 2. *Secret key rate per pulse.* Performance versus a) distance in the case of fixed visibility, $V = 0.9$, and b) visibility at a channel length of $L = 100$ km. For each of the three protocols, an optimization was performed with respect to the mean photon number μ (see supplementary material). Parameters: $\eta_d = 0.1$, $p_d = 10^{-7}$, $\alpha_{loss} = 0.2$ dB/km, and $p_{decoy} = 0.02$ for COW and DPTS.

in four consecutive pulses. It follows that Eve's states conditioned on Alice's preparation are

$$\begin{aligned}
 \rho_{E|0} &= \frac{1}{2} (P_{+\alpha_E, \text{vac}, +\alpha_E, \text{vac}} + P_{-\alpha_E, \text{vac}, -\alpha_E, \text{vac}}), \\
 \rho_{E|1} &= \frac{1}{2} (P_{+\alpha_E, \text{vac}, -\alpha_E, \text{vac}} + P_{-\alpha_E, \text{vac}, +\alpha_E, \text{vac}}), \\
 \rho_{E|2} &= \frac{1}{2} (P_{\text{vac}, +\alpha_E, \text{vac}, +\alpha_E} + P_{\text{vac}, -\alpha_E, \text{vac}, -\alpha_E}), \\
 \rho_{E|3} &= \frac{1}{2} (P_{\text{vac}, +\alpha_E, \text{vac}, -\alpha_E} + P_{\text{vac}, -\alpha_E, \text{vac}, +\alpha_E}),
 \end{aligned} \tag{6}$$

where P_x is the projection operator. To calculate the maximum accessible information for Eve, it is helpful to

define $\gamma = e^{-|\alpha_E|^2}$. By this convention the overlaps between states can be written as $|\langle +\alpha_E, \text{vac}, +\alpha_E, \text{vac} | -\alpha_E, \text{vac}, -\alpha_E, \text{vac} \rangle| = \gamma^4$, and $|\langle j|k \rangle| = \gamma^2$ for $j \neq k$, where $j, k \in \{0, 1, 2, 3\}$. From this, the Holevo quantity [Eq. (5)] becomes

$$\begin{aligned}
 \chi_{AE}^{(0)} &= -\frac{(1+\gamma^2)^2 + (2\gamma)^2}{8} \log_4 \left[\frac{(1+\gamma^2)^2 + (2\gamma)^2}{8} \right] \\
 &\quad - \frac{3(1-\gamma^2)^2}{8} \log_4 \left[\frac{(1-\gamma^2)^2}{8} \right] \\
 &\quad - \frac{1-\gamma^4}{2} \log_4 \left(\frac{1-\gamma^4}{8} \right) + h_4 \left(\frac{1-\gamma^4}{2} \right).
 \end{aligned} \tag{7}$$

where S_4 is defined below Eq. (3), and $h_4(x) = S_4(x) + S_4(1-x)$. Equation (7) presents an upper bound on the information Eve can obtain by trying to distinguish between the four different states. However, Eve can do better than this by trying to establish *partial* information about the state Alice and Bob agreed upon. Specifically, by performing measurements on the sub-blocks which are temporally adjacent to the time slots in which Alice and Bob agreed on the bit pairs, Eve may with some probability infer that the state was either of the pairs $|0\rangle, |1\rangle$ or $|2\rangle, |3\rangle$ (in this case, Eve has no way of knowing the phase-related bit). Since this additional attack by Eve is conditioned on her *not* getting a conclusive result in the primary measurement, the corrected Holevo quantity becomes

$$\chi_{AE} = \chi_{AE}^{(0)} + (1 - \chi_{AE}^{(0)}) \chi_{AE}^{(1)}, \tag{8}$$

where $\chi_{AE}^{(1)}$ is derived and given in the supplementary material. Note however, that Eve is essentially ignorant about the position of block separations. Therefore making conclusions from this secondary attack will result in errors for Eve.

Numerical results

Combining the results of the previous sections [in particular Eqs. (2), (4), and (8)] enables us to plot a first upper bound on the secret key rate under the assumption of collective attacks. Specifically, Fig. 2 shows R_{sk} versus communication distance at the optimized values of the mean photon number μ . To assess the performance of the DPTS protocol, we have included plots for both COW and DPS. In comparison, the DPTS protocol has a similar performance as the other protocols under the realistic condition of non-ideal visibilities (as examples we have used $V = 0.9$ and $V = 0.95$). Noteworthy, the DPTS protocol displays a less critical dependence on the visibility when compared to the DPS protocol.

In a more realistic situation, the comparison of the protocols must take into account the detector dead times.

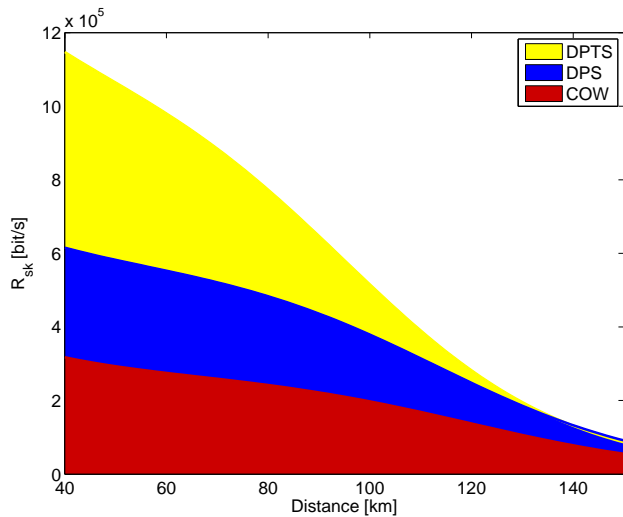


FIG. 3. *Secret key rate in real case scenario.* Different secret key rates achievable in a medium-length link scenario, where the detector dead times play an important role. We use mean photon numbers for the different protocols of $\mu_{DPTS} = 0.23$, $\mu_{DPS} = 0.19$, and $\mu_{COW} = 0.52$, at repetition rate $\nu = 10 \cdot 10^9$ Hz, and fixed block length of $N = 4$. The detectors are specified by dark-count probability $p_d = 3.5 \cdot 10^{-9}$, a dead time of $t_d = 1 \cdot 10^{-6}$ s, and efficiency $\eta_d = 0.1$. We assume $V = 1$, and a decoy-sequence probability of $p_{decoy} = 0.02$ for COW and DPTS.

For example, considering the case of commercial InGaAs infrared single-photon detectors (the most used in fiber links and the most promising thanks to the non-cryogenic requirement), they generally exhibit a dead time in excess of $1 \mu\text{s}$ [23, 24]. Thus, in any scenario where the detector dead time significantly influences the key generation rate, the ability to extract two bits of information per detection event grants the DPTS protocol an advantage. To illustrate this effect, Fig. 3 shows an example of the secret key rate in bits s^{-1} , after inclusion of the dead-time dependency.

DISCUSSION

The main figure of merit in a QKD system is the achievable secret key rate. Therefore, to assess the performance of DPTS, Fig. 2 displays this quantity for DPTS in comparison with the standard COW and DPS protocols. Evidently, the comparison shows very similar behavior of the three DPR protocols. Considering more specifically the case of DPTS, the final key rate is influenced by the length of the blocks N prepared by Alice. Even though a higher value of N allows an increased sifted key rate, it is necessary to consider a trade-off between the length of blocks and the information leakage to Eve. In the case of long-distance links (in excess of 100 km), the behavior of

the three protocols is maintained, but as the DPTS protocol is more severely influenced by dark count events, it is generally limited to shorter distances. On the other hand, as seen by comparing the subfigures of Fig. 2, the DPTS protocol is less dependent on the interferometer visibility. This fact permits the proposed protocol to achieve a more stable secret key generation rate in comparison with the DPS protocol. In implementing a QKD protocol, it is necessary to consider the limitations set by the optical and electronic devices [25–27]. An important example is the single-photon detector dead time t_d , which sets an upper limit on the key generation rate. This parameter is important in a short- or medium-length link scenario, where the average wait time between detection events is of the same order of magnitude as t_d (which is typically on the order of microseconds). In Fig. 3, it is shown that DPTS may achieve a significant increase in the secure key rate at distances where the detector dead time is a limiting factor. This potential arises due to the ability of the DPTS protocol to extract two bits of information per detection event. The use of multiple degrees of freedom in transmission of information, intuitively increases the complexity of the scheme in comparison with protocols dealing with each individual degree of freedom. Despite DPTS not being an exception to this rule of thumb, the complexity overhead in comparison to DPS or COW is not crucial. On the other hand, DPTS does exhibit two significant practical advantages. Firstly, the COW protocol requires a monitoring line to check for the presence of an eavesdropper. However, such a monitoring line is unnecessary for DPTS, as an interferometer is directly used in the data line, and hence implements the necessary coherence check. Thus, the decrease in rate related to monitoring of the data line in COW, is not a limitation for DPTS. Secondly, the stability of the interferometer over time, is a considerable challenge in implementations of the DPS protocol in non-stable environments. The performance of the DPTS protocol is inherently more resilient against fluctuating interferometer visibilities, because the temporal bit remains unaffected by such inefficiencies. This entails, that DPTS might be better suited in cases where it is difficult to maintain the interferometer visibility above a certain required operation threshold. Finally, DPTS can potentially play an important role in QKD networks spanning from metropolitan to intercity distances [28–30]. Interestingly, the required measurement apparatus is identical to the one used in DPS, and in fact, the receiver does not need to know *a priori* whether the signals arise from a DPS or a DPTS encoding. This compatibility suggests that a versatile network encompassing the use of both the DPS and DPTS protocols is feasible.

In conclusion, we have proposed a novel kind of distributed-phase-reference protocol for quantum key distribution. Utilizing both the time- and phase degrees of freedom, this protocol provides a significant step towards

realization of fast, reliable, and practical quantum communication. Future directions include a finite-key analysis and a real-time field implementation.

ACKNOWLEDGEMENTS

We would like to thank Dr. Giuseppe Vallone and Dr. Davide. G. Marangon of Department of engineering information (DEI), University of Padova for the useful discussions and for the insightful comments.

Our work was supported by the DNRF Research Centre of Excellence, SPOC (Silicon Photonics for Optical Communications), ref. DNRF123.

AUTHOR CONTRIBUTIONS STATEMENT

D.B conceived the work. D.B., J.B.C, M.A.U. and Y.D. obtained the conceptional main results. J.B.C provided security proof. J.B.C, S.R. and D.B formulated information theory analysis. K.R and L.K.Ø supervised the project. All authors discussed the results and contributed to the final manuscript.

- [16] K. Inoue, T. Honjo, *Physical Review A - Atomic, Molecular, and Optical Physics*, **71**(4) (2005)
- [17] W. Buttler, S. Lamoreaux, et al., *Physical Review A*, **67**(5)(2003)
- [18] V. Martin, *arXiv* 1407.3257v1 (2014)
- [19] C. H. Bennett, G. Brassard, et al., *IEEE Transactions on Information Theory*, **41** (1995)
- [20] A. M. Nielsen, L. I. Chuang, *Quantum Computation and Quantum Information* (2000)
- [21] C. Branciard, N. Gisin, et al., *New Journal of Physics*, **10**. (2008)
- [22] I. Devetak, A. Winter, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, **461**(2053) (2005)
- [23] R. H. Hadfield, *Nature Photonics*, **3**(12) (2009)
- [24] A. Tosi, N. Calandri, et al., *IEEE J. Sel. Top. Quantum Electronics*, **20** (2014)
- [25] P. Sibson, C. Erven, et al., *ArXiv* 1509.00768 (2015)
- [26] E. Diamanti, H. Takesue, et al., *Optics Express*, **14**(26) (2006)
- [27] H. Takesue, E. Diamanti, et al., *Optics Express*, **14**(20) (2006)
- [28] M. Sasaki, M. Fujiwara, et al, *Optics Express*, **19**(11) (2011)
- [29] B. Fröhlich, J. F. Dynes , et al., *Nature*, **501**(7465) (2013)
- [30] M. Peev, C. Pacher, et al., *New Journal of Physics*, **11**(7) (2009)

* dabac@fotonik.dtu.dk

- [1] C. H. Bennet and G. Brassard, *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984).
- [2] G. Vallone, D. Bacco, et al., *Phys. Rev. Lett.*, **115** 040502 (2015)
- [3] B. Korzh, C. C. W. Lim, et al., *Nature Photonics*, **9**(3) (2015).
- [4] D. Bacco, M. Canale, et al., *Nature Communications*, **4**, 1–8. (2013)
- [5] L. Ji, J. Gao, et al., *ArXiv* 1602.05047 (2016)
- [6] H. Takesue, T. Sasaki, et al., *Nature Photonics*, **9**(12), (2015)
- [7] M. Mirhosseini, O. S. Magaña-Loaiza, et al., *New Journal of Physics*, **17**(3), (2015)
- [8] M. A. Usuga, C. R. Mueller, et al., *Nature Physics*, **6**(10) (2010)
- [9] N. Gisin, G. Ribordy, et al., *Reviews of Modern Physics*, **74**(1), (2002)
- [10] V. Scarani, H. Bechmann-Pasquinucci, et al., *Reviews of Modern Physics*, **81** (3) (2009)
- [11] G. Brassard, N. Lütkenhaus, et al., *Phys. Rev. Lett*, **85**(1) (2000).
- [12] V. C. Usenko, B. I. Lev, et al, *Physics Letters, Section A: General, Atomic and Solid State Physics* **348**(1-2) (2005)
- [13] K. Inoue, E. Waks, et al., *Physical Review A*, **68**(2), 022317 (2003)
- [14] D. Stucki, N. Brunner, et al. *Applied Physics Letters*, **87**(19), (2005)
- [15] N. Gisin, G. Ribordy, et al., *arXiv* 0411022v1, (2004)

ADDITIONAL INFORMATION

Eve's additional attack

We here explore an additional (or secondary) attack option which is available to Eve when performing the beam-splitting attack (BSA). The possibility of this additional attack, arises as Alice repeats the temporal sequence (i.e. non-empty, empty or empty, non-empty) within each block of length N . To clarify, assume that Bob has a detection event in a certain time slot. Eve, wanting to know which state Alice prepared for Bob, extracts the corresponding 4-pulse state from her quantum memory, and tries to determine whether it was $|0\rangle, |1\rangle, |2\rangle$ or $|3\rangle$ (See Main Text, Security analysis). Often, Eve has an inconclusive measurement and the state of the 4-pulse system is destroyed. However, in these cases, she can extract an adjacent 2-pulse state from her quantum memory, and try to learn its temporal encoding (i.e. is it $|0\rangle, |1\rangle$ or $|2\rangle, |3\rangle$), which is worth 1 bit of information. Unfortunately for Eve, this bit will not always be correct: In some cases she extracts a 2-pulse state belonging to an adjacent block of the opposite temporal encoding. And, essentially for the protocol, she does not know when this is the case due to the randomized block length.

The probability of a correct bit for Eve p_E , depends on the average block size $\langle N \rangle$, and can found to satisfy (assuming a negligible fraction of decoy sequences)

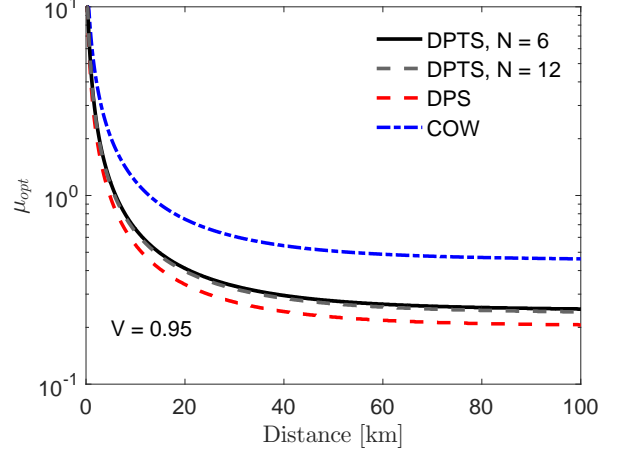
$$p_E = \frac{\langle N \rangle - 2}{\langle N \rangle - 1}, \quad \langle N \rangle \geq 4, \quad (9)$$

which tends towards unity for $\langle N \rangle \gg 4$ as intuitively expected. Since the nature of the errors are identical to those of a binary symmetric channel (BSC), we can explicitly express the correction term in Eq. (8) as

$$\chi_{AE}^{(1)} = \frac{1}{2} \left[1 - h_2(p_E) \right] \left[S_4 \left(\frac{1 + 3\gamma^2}{4} \right) + 3 S_4 \left(\frac{1 - \gamma^2}{4} \right) - h_4 \left(\frac{1 - \gamma^2}{2} \right) \right]. \quad (10)$$

The pre-factor of $1/2$ enters since this attack only gives half of the state information, the factor $1 - h_2(p_E)$ is the BSC capacity, and finally the three terms in the last square bracket results from analyzing how well Eve can discriminate unambiguously between the two different temporal sequences. Note that this is not identical to the expression for the coherent-one-way protocol (see [21]), since Eve's conditioned states in our case are: $\rho_{E|\text{vac}} = (P_{+\alpha E, \text{vac}} + P_{-\alpha E, \text{vac}})/2$ and $\rho_{E|1} = (P_{\text{vac}, +\alpha E} + P_{\text{vac}, -\alpha E})/2$.

The corrected Holevo bound presented in this section only takes into account a single additional measurement performed by Eve. In principle, this measurement may be inconclusive in which case she can extract a new 2-pulse



Additional Figure 1. *Optimal μ versus distance.*

state and perform a new measurement. Thus, a more accurate analysis does exist, but is considered outside the scope of this paper as it is not expected to have a crucial impact on the bound for $\langle N \rangle \leq 8$.

Mean photon number parametrization

The secret key rate R_{sk} in Eq. (2) indicates that one should always try to optimize $I_{AB} - \min(I_{AE}, I_{AB})$ with respect to the free variables available. For a given transmission link, an obvious parameter to optimize is the mean photon number per pulse μ . In general, Bob's detection rate increases with μ , but so does Eve's probability of measuring the corresponding state. Thus, for a specific setup (QKD protocol, transmission channel, interferometer, detectors, etc.), it is expected that an optimal value, μ_{opt} , exists. As an example, Fig. 1 shows the behavior of μ_{opt} versus transmission distance. These values were, for each transmission distance, obtained by numerically finding the value μ_{opt} , which optimized R_{sk} [which is then shown in Fig. 2]. As the DPTS protocol forces a potential to distinguish both between states $|+\alpha\rangle, |-\alpha\rangle$ (as in DPS) and $|\pm\alpha\rangle, |\text{vac}\rangle$ (as in COW) it is perhaps not surprising that the optimal value μ_{opt} for the DPTS protocol lies somewhere in between the corresponding optimal values for DPS and COW.